FS-20131217.04B

Forum Standaardisatie

Bezoekadres:
Wilhelmina v Pruisenweg 52
2595 AN Den Haag
96810
2509 JE Den Haag
www.logius.nl

Inlichtingen bij
B.S.J. Knubben
Senior Adviseur
M +31(0)6-21162373
bart.knubben@logius.nl

Datum
30 oktober 2013

notitie

Reactie op "ON2013 Algemene Functionele Beschrijving" d.d. 3 september 2013 [versie 1.0]

1. Achtergrond

Sinds enkele jaren maakt een groot aantal overheidsorganisaties gebruik van gezamenlijk aanbestede overeenkomsten op het gebied van tele- en datacommunicatie. Eén van deze overeenkomsten betreft de overeenkomst voor vaste dataverbindingen, bekend onder de naam OT2006-Vaste Data. De raamovereenkomst loopt in oktober 2013 af.

Om zorg te dragen voor opvolging voor deze aflopende overeenkomst en om nieuwe initiatieven op het gebied van datacommunicatie mogelijk te maken, is het project ON2013 opgestart. ON2013, staat voor 'OverheidsNetwerken 2013'. ON2013 is bestemd voor ministeries, inclusief agentschappen, en Zelfstandige Bestuursorganen (ZBO's).

Het project ON2013 werkt aan het opstellen van de aanbestedingsdocumenten. De voorlopige inzichten inzake de behoefte zijn vastgelegd in het document "ON2013 Algemene Functionele Beschrijving", d.d. 3 september 2013 (hierna: ON2013-document). Het project heeft via een consultatie aan de markt gevraagd om op het document te reageren.

Het Forum Standaardisatie is gevraagd om ook een reactie te geven. Een dergelijk reactie past bij de ambitie van het Forum Standaardisatie om meer pro-actief te adviseren over standaarden en interoperabiliteit bij grote ICT-investeringen door de overheid. Deze notitie betreft de reactie van het Forum Standaardisatie.

2. Aanpak en opzet

De scope van de reactie omvat het werkdomein van Forum Standaardisatie, namelijk standaarden en interoperabiliteit. Vanwege deze scope lag de focus van de review op de paragrafen met technische eisen (2.5 en 3.4), waarin de standaarden voor gegevensuitwisseling terugkomen.

Bij het opstellen van het advies zijn twee experts uit het netwerk van het Forum Standaardisatie betrokken, namelijk Niels den Otter (manager netwerkdiensten, SURFnet) en Marco Davids (technisch adviseur, SIDN). SURFnet heeft ook zijn laatste RFP-document voor upstream Internet-connectiviteit beschikbaar gesteld. Omwille van de voortgang zijn de opmerkingen en documentatie van de experts eerder onverkort, in ruwe vorm, doorgestuurd naar het projectteam van ON2013.

Deze notitie is opgesteld door het Bureau Forum Standaardisatie. In deze notitie

zijn de opmerkingen van de experts geordend, verduidelijkt en aangevuld.

Het Forum Standaardisatie heeft in de vergadering op 29 oktober ingestemd met dit adviestraject. Tijdens de vergadering op 17 december zal deze notitie worden geagendeerd.

De eerstvolgende paragraaf bevat algemene opmerkingen over het document "ON2013 Algemene Functionele Beschrijving" vanuit de scope van standaarden en interoperabiliteit. In de paragraaf daarna staan de relevante standaarden van de lijsten van het Forum Standaardisatie centraal. In de laatste paragraaf van deze reactie volgen relevante opmerkingen per eis of onderdeel van het ON2013-document.

3. Algemene opmerkingen

- Het Forum Standaardisatie juicht het toe dat ON2013 een publieke consultatie uitvoert. Het is voor het Forum Standaardisatie, maar ook voor andere partijen, een uitstekende gelegenheid om expertise in te brengen en vroegtijdig gericht advies te geven.
- Het verdient aanbeveling om in de documenten expliciet te refereren aan het open standaarden-beleid van de overheid, zodat dit kader ook voor marktpartijen kenbaar is. Zie daarvoor ook de generieke bestekteksten voor open standaarden.[1] Bijv. iets in de trant van: *"Het kabinet stelt open standaarden als norm. Voor de (semi-)publieke sector geldt sinds 2009 het 'pas toe of leg uit'-regime. Overheden zijn verplicht om bij de aanschaf van ICT-systemen/-diensten te kiezen voor de relevante standaarden van de 'pas toe of leg uit'-lijst. De aanbesteding van ON2013 is in lijn met dit open standaarden-beleid."*
- In het document worden verschillende standaarden bij naam genoemd. Dat is op zichzelf goed. Om misverstanden te voorkomen is het echter aanvullend van belang om telkens expliciet te maken om welke versie wordt gevraagd en te verwijzen naar de relevante specificatiedocumenten. In dit geval zijn dat veelal zogenoemde RFC's van de nationale standaardisatieorganisatie Internet Engineering Task Force (IETF).
- Informatiebeveiliging is een belangrijk aspect van interoperabiliteit en uiteraard ook van belang voor ON2013. Voor zover dat nog niet is gebeurd, verdient het aanbeveling om specialisten, bijv. van het NCSC en Nationaal Bureau voor Verbindingsbeveiliging (NBV), te vragen om advies.

4. Relevante standaarden

De onderstaande standaarden van de 'pas toe of leg uit'-lijst (http://forumstandaardisatie.nl/ptolu) zijn mogelijk relevant voor ON2013. Telkens is aangegeven of de desbetreffende standaard in het ON2013-document is genoemd. En, zo ja, waar deze staat genoemd en, zo nee, waarom deze relevant kan zijn.

Standaard	Korte beschrijving	In ON2013-doc?	Opmerking
IPv4 en IPv6	Internetnummers	Ja	Zie: par. 3.4, eisen 1.07 – 1.09 en par. 5.2 eisen 5.3 -5.5. Een aandachtspunt is dat op verschillende andere plekken IP wordt genoemd, zonder expliciet versies te noemen.

[1] Zie: https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/1217/20130326-Generieke-bestekteksten-open-standaarden-v1.12.pdf

ISO27001 en 27002	Informatiebeveiliging	Ja	Zie: par. 4.3, eis 11.2. Aandachtspunt is dat de Baseline Informatiebeveiliging Rijk (BIR), die op deze normen is gebaseerd en specifieker is, niet wordt genoemd.
DNSSEC	Beveiliging van domeinnamen	Nee	Relevant als bij de internetdienst ook resolvers worden verwacht. Hoewel dat niet het geval lijkt, noemen we deze standaard hier zekerheidshalve.
DKIM	Mail-authenticatie	Nee	Relevant als bij de internetdienst ook mail-relay's worden verwacht. Hoewel dat niet het geval lijkt, noemen we deze standaard hier zekerheidshalve.
ODF	Documenten	Ja	Zie: par. 4.3, eis 8.8
PDF/A	Documenten	Nee	Zie: par. 4.3, eis 8.8

De onderstaande standaarden van de lijst met gangbare standaarden (http://forumstandaardisatie.nl/gangbaar) zijn mogelijk relevant voor ON2013. Ook bij deze standaarden is telkens aangegeven of de desbetreffende standaard in het AFB is genoemd.

Standaard	Korte beschrijving	In ON2013-doc?	Opmerking
TCP/IP	Netwerken, transportprotocol	Ja	Zie: par. 2.5, eis 5.14
SNMP	Netwerken, managen apparatuur	Ja	Zie: par. 3.4, eis 1.06 en par. 2.5, eis 5.20
DHCP	Netwerken, configureren van hosts	Ja	Zie: par. 2.5, eis 5.16
IPsec	Beveiliging van IP-verbindingen	Nee	Mogelijk relevant voor par. 2.5, eis 5.19
NTP	Netwerken,synchroniseren tijd	Nee	O.a. belangrijk voor log-files.
SHA-2	Hash-algoritme	Nee	Mogelijk relevant voor par. 2.5, eis 5.19
UDP	Netwerken, transportprotocol	Ja	Zie: par. 2.5, eis 5.14
AES (in behandeling voor opname op lijst)	Encryptie-algoritme	Nee	Mogelijk relevant voor par. 2.5, eis 5.19

5. Opmerkingen per eis/onderdeel

De tabellen hieronder bevatten opmerkingen per eis of onderdeel van het ON2013-document . Daarbij is de ordening van de ON2013-document aangehouden.

2. Connectiviteitsdiensten

2.4 Bandbreedtes

Hier ligt niet de primaire focus van de reactie van het Forum. Voor de volledigheid zie de separaat toegestuurde opmerkingen van SURFnet en SIDN.

2.5 Technische eisen

#	Eis uit ON2013-document	Opmerking
1.3	Al het verkeer dient transparant, ongefilterd en ongelimiteerd getransporteerd te worden.	1. Je zou hier kunnen lezen dat geen NAT mag worden toegepast. Dat is waarschijnlijk niet de bedoeling 2. Bij link-bundling (zie eis 4.4) is dat voor LACP wellicht niet gewenst. Mogelijk oplossing 'te worden'=>'te kunnen worden'.
1.5	De opdrachtnemer dient een verhoogde beschikbaarheid te kunnen aanbieden middels oplossingen via geografisch gescheiden fysieke infrastructuurpaden, van één of twee opdrachtnemerlocaties naar één of twee deelnemerlocaties.	Zijn de services niet altijd end-to-end en is daarmee niet veel belangrijker dat de volledige paden tussen deelnemerlocaties redundant zijn? Zo ja, ergens vragen dat de service vanuit twee opdrachtnemerlocaties niet verder in het netwerk weer bij elkaar komt.
1.6	De opdrachtnemer dient als oplossing voor de verhoogde beschikbaarheid 'dual- routed, multi-homed' aan te kunnen bieden. 'Dual-routed, multi-homed' is het redundant ontsluiten van een locatie van de deelnemer via geografisch gescheiden fysieke infrastructuurpaden naar twee verschillende aansluitlocaties van de opdrachtnemer.	Hoe is dit anders dan 1.5? Is dat daar geen deel van.
1.7	De opdrachtnemer dient een end-to-end Quality-of-Service mogelijk te maken, gebaseerd op de ITU-T Y.1541 standaard.	1. Is ITU-T Y.1541 voor alle genoemde koppelingen relevant (if at all)? Deze standaard gaat over 'Network performance objectives for IP-based services'. Is het voor de Ethernet (VPN) gebaseerde diensten niet relevanter om naar MEF Carrier-Ethernet standaarden te verwijzen? 2. Dit lijkt haaks te staan op eis 1.3.
1.8	De diensten van opdrachtnemer vormen geen beperking voor deelnemers om door middel van zijn eigen IP/netwerkapparatuur IP-VPN's te creëren met CoS en/of QoS (aansluiting is IP-transparant).	Wordt verwacht dat de opdrachtnemer niets doet op basis van de DSCP-waarde in het IP-pakket? Of juist wel, omdat gesteld wordt dat IP-VPNs met CoS/QoS gecreëerd kunnen worden?
1.9	De opdrachtnemer garandeert dat over de aangeboden diensten, toepassingen zoals VoIP en real-time (multicast) video (of minimaal vergelijkbaar) getransporteerd kunnen worden.	Multicast is een apart onderwerp en komt in andere eisen (4.8 en 4.9) ook terug. Wellicht hier verwijzen naar de desbetreffende specifieke eisen.
1.10	Vaste datacommunicatiediensten dienen geschikt te zijn voor het end-to-end- transport van VoIP.	Is dit anders dan 1.9?
4.1	De aangeboden ethernet	1522 bytes tegenstrijdig met 4.2? Leest nu

#	Eis uit ON2013-document	Opmerking
	frames (zowel de ethernet header als de ethernet data) worden zonder aanpassingen bij de bestemming afgeleverd. De dienst is transparant voor extra headers voor o.a. ISL, 802.1q, q-in-q, MPLS labels. Tagged frames tot 1522 bytes moeten worden ondersteund.	vreemd. Anders duidelijk maken dat 1522 bytes altijd ondersteund moet worden op UNI en dat op verzoek deelnemer de MTU tot maximaal … bytes opgehoogd moet kunnen worden. Notatie; 802.1q => 802.1Q, q-in-q => Q-in-Q (802.1ad).
4.2	Jumbo frames (ethernet frames tot 9180 bytes) worden ondersteund.	Ter informatie: SURFnet houdt 9000 bytes aan voor 'klant' jumbo frames. In backbone is MTU uiteraard altijd hoger dan dat.
4.3	IEEE 802.1ad (Q-in-Q) dient ondersteund te worden.	Wat wordt hier gevraagd? Dat de service transparant is voor Q-in-Q frames? Dat is gelijk aan transparantie in 4.1?
4.4	Linkaggregatie op basis van IEEE 802.3ad dient ondersteund te worden.	Is LACP hier wens/must? Of is statisch de standaard? Daarnaast is het hier waarschijnlijk de vraag om dit te ondersteunen op de koppeling tussen aanbieder/deelnemer en niet dat de service transparant is voor bijv. LACP. Duidelijker opschrijven.
4.5	Opdrachtnemer dient decentraal minimaal 20 en centraal minimaal 1000 VLAN's op één locatie te kunnen leveren.	Ook nog eisen aan minimaal aantal MAC adressen per lokatie / E-LAN? Of wordt alles op routers getermineerd.
4.7	Opdrachtnemer dient de verschillende VLAN's op één locatie logisch gescheiden af te leveren binnen één fysieke interface.	Dus 802.1Q standaard moet ondersteund. Verder; af te leveren => af te kunnen leveren. Anders in strijd met 4.6. 'binnen een fysieke interface' => 'op een fysieke interface' (zoals 4.6).
4.8	Opdrachtnemer ondersteunt "ethernet multicasting".	1. Wat is dit? Transparantie voor ethernet multicast frames? Of wordt hier meer gevraagd, bijv in E-LAN omgeving? Daarnaast kan het goed zijn ergens performance eisen hieraan te stellen als er veel multicast verkeer gebruikt gaat worden voor specifieke applicaties. 2. Het gaat hier waarschijnlijk om IP Multicast. Dit werkt net even anders bij IPv4 dan bij IPv6. Bij IPv4 is het eigenlijk een addon terwijl het bij IPv6 een geïntegreerd onderdeel is. Naar relevante RFC's verwijzen. Zie o.a.: http://en.wikipedia.org/wiki/IP_multicast#Routing
4.9	Opdrachtnemer ondersteunt "ethernet multicasting", waarbij multicast-verkeer alleen wordt aangeboden op interfaces die aangemeld zijn voor de multicast- groep.	Hier wordt waarschijnlijk bedoeld dat de aanbieder IGMP (versie 2) snooping ondersteund. Zeker stellen dat IGMPv3 (in toekomst) niet nodig is. Of MLDv2 voor IPv6.
4.13	Ethernet unicast verkeer wordt alleen aangeboden op interface waarop betreffende MAC-adres bereikbaar is.	'Bereikbaar' is voor aanbieder lastig te bepalen. 'Geleerd' of 'Aktief' beter volgens mij. Gaat om MAC-learning. Is dit alleen op E-LAN gewenst of ook op E-LINE diensten.
5.1	Kenmerk van de IP-VPN-dienst is dat een VPN zich	1. Niet direct duidelijk waar de 2 interfaces eis op duidt. Klant en backbone? Of altijd minimaal

#	Eis uit ON2013-document	Opmerking
	gedraagt als een gesloten netwerk en het verkeer binnen dit VPN niet over internet wordt getransporteerd. De IP-VPN-dienst bestaat uit de volgende componenten: - accesslijn in diverse bandbreedtes tussen locatie van een deelnemer en het netwerk van opdrachtnemer (inclusief poort op het netwerk van opdrachtnemer); - beheerde apparatuur met minimaal twee interfaces.	2 interfaces voor de afnemer beschikbaar? In dat geval waarom deze eis (heeft invloed op kosten) en niet een upgrade scenario gebruiken voor lokaties waar nodig. 'beheerde apparatuur' is ook een ruim begrip. Door wie beheert? Moet deze op locatie van de afnemer staan? 2. O.b.v. welke standaarden werkt de IP-VPN-dienst: Bijv. MPLS en IPsec? RFC4364?
5.3	Opdrachtnemer dient IPv4 te ondersteunen.	Van belang om te verwijzen naar relevante achterliggende RFC's voor de standaarden. Zie RIPE 554, http://www.ripe.net/ripe/docs/ripe-554 en zie NL vertaling van RIPE 554, http://www.forumstandaardisatie.nl/fileadmin/os/publicaties/ripe-554-nl.pdf
5.4	Opdrachtnemer dient IPv4 / IPv6 conversie te ondersteunen.	1. Zie opmerkingen onder eis 5.3 2. Wat is dit binnen een IP-VPN? Wordt hier om een tunnel broker gevraagd? Of NAT64 / NAT46? Dit is niet duidelijk.
5.5	Opdrachtnemer dient IPv6 te ondersteunen.	Duidelijk maken dat dat geldt voor alle protocollen die in dit blok genoemd worden. Dus waar mogelijk ook voor de routeringsprotocollen.
5.7	Opdrachtnemer dient op het koppelvlak per aansluiting IS-IS-, (E)IGRP- en BGP-4-routering te ondersteunen.	1. Verwijzen naar relevante RFC, bijv. RFC1142 2. Is (E)IGRP een harde eis als PE-CE routeringsprotocol? Dit is een Cisco proprietary protocol en wellicht niet door elke aanbieder ondersteund (?).
5.10	Opdrachtnemer dient op de aangesloten locaties meerdere VPN's (gebundeld op de aanwezige fysieke interfaces) te kunnen leveren. Het aantal te leveren VPN's is op een decentrale lokatie is maximaal 20 VPN's, op de centrale lokatie is het aantal te leveren VPN's maximaal 256 (gebundeld over de fysieke interfaces).	Scheiding waarschijnlijk op basis van VLAN-tag; dus 802.1Q ondersteund op koppelvlak om VPNs apart aan te kunnen leveren.
5.12	Opdrachtnemer dient de verschillende VPN's op één aangesloten locatie logisch gescheiden af te kunnen leveren binnen één fysieke interface.	Wordt dit niet al gedekt met 5.9 en 5.11?
5.13	De aanbieder dient in een IP VPN dienst Quality of Service te ondersteunen. Er moeten ten minste 5 verschillende verkeersklassen gedefinieerd kunnen worden. […]	100 ms delay in Nederland is gigantisch. Een 20 ms jitter lijkt mij te hoog voor 'real-time/low jitter' applicatie. 10 ms(RTT, dus heen en terug) moet kunnen, maar voor aanbieders is 20 ms als harde eis misschien veiliger. Goed om hier met aanbieders over te praten / SLAs te bestuderen. Idem voor jitter. Mooiste zou zijn, als dit onder 1 ms kan, maar niet zeker

#	Eis uit ON2013-document	Opmerking
	- Klasse 5 (best effort) Al het overige verkeer wordt aan deze klasse toegewezen.	dat aanbieders zich hieraan durven te committeren.
5.14	Classificatie van verkeer in verkeersklassen dient mogelijk te zijn op: - source-interface; - source IP-adres; - destination IP-adres; - TCP/UDP-poortnummer; - IP-protocolnummers; - diffserv: DSCP/TOS-veld; - combinaties van bovenstaande.	Als IPv6 hier eis is, zou ik dat noemen. Of ergens opschrijven dat IP = IPv4 En IPv6. In de praktijk kan dit wellicht probleem zijn. Haalbaarheid en hardheid eis checken.
5.16	Opdrachtnemer dient de DHCP-relay functionaliteit te ondersteunen.	Ook hier geldt dat deze IPv6 moet ondersteunen (DHCPv6). Verder niet helemaal duidelijk hoe dit relevant is in L3/IP-VPN. Wat wordt hier gevraagd?
5.17	Opdrachtnemer dient de mogelijkheid van het koppelen met externe netwerken te ondersteunen.	Niet duidelijk. Wordt hier gevraagd om ook Internet-toegang vanuit een VPN mogelijk te maken? Of om meerdere VPNs onderling te koppelen?
5.18	Toegangsbeveiliging tot integrale netwerken dient mogelijk te zijn op basis van access listen. Het moet in ieder geval mogelijk zijn om verkeer op basis van bron- en bestemmingsadressen, protocollen of een combinatie daarvan te blokkeren of juist expliciet toe te staan. Tevens dient reverse-path-controle ondersteund te worden.	1. Ook uRPF ingress filtering moet kunnen (en moet zelfs default aangezet zijn). Zie BCP38/RFC2827 en RFC3704. 2. Met 'reverse-path-controle' wordt waarschijnlijk gedoeld op 'strict mode uRPF'. En/of ook de feasible/loose variant?
5.19	De versleuteling die wordt toegepast bij Internet VPN's dient minimaal gebaseerd te zijn op 3DES of een beter versleutelingsalgoritme.	1. O.b.v. welke standaarden werkt de IP-VPN-dienst: Bijv. MPLS en IPsec? RFC4364? 2. Zou je hier niet tenminste om de gangbare open standaard AES moeten vragen? Is daarnaast SHA-2 hier niet relevant? 3. Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) adviseert en doet de keuring van beveiligingsproducten (o.a. voor netwerkbeveiliging) voor inzet door de Rijksoverheid: https://www.aivd.nl/organisatie/eenheden/nationaal-bureau/artikel/goedgekeurde/#Netwerkbeveiliging
5.20	Opdachtnemer dient SNMP-toegang tot eindapparatuur op de Aansluitpunten voor monitoring en het uitlezen van gebruiksstatistieken te ondersteunen.	1. Relevante RFC voor SNMP noemen 2. NCSC beveelt SNMPv3 (RFC3411 t/m RFC 3418, ook wel bekend als STD0062) aan en doet een aantal andere beveiligingsmaatregelen aan: https://www.ncsc.nl/actueel/nieuwsberichten/netwerken-kwetsbaar-door-onveilige-snmp-configuratie.html 3. SNMPv3 staat op de lijst met gangbare standaarden: https://lijsten.forumstandaardisatie.nl/open-

#	Eis uit ON2013-document	Opmerking
		standaard/snmp 4. De ervaring van SURFnet bij IP upstream inkoop is dat aanbieders dit niet meer (zomaar) toestaan. De apparatuur wordt vaak ook voor andere klanten gebruikt en afscherming is dan op zijn minst lastig.

3. Internettoegang

3.2 Dual provider strategie

Tekst uit ON2013-document	Opmerking
Voor enkele locaties geldt dat de beschikbaarheid van internettoegang zodanig belangrijk is dat er voor wordt gekozen deze locaties via twee verschillende opdrachtnemers op het internet aan te sluiten.	1. Van belang dit nauwkeuriger te definiëren. Denk aan netwerk-topologische scheidingen op basis van verschillende AS-en, maar ook; fibers die via gescheiden paden het pand binnenkomen. 'verschillende opdrachtnemers' is te vaag. 2. Afhankelijkheid van netwerk-routering is ook een vereiste. Verkeer tussen A en B, beiden in Nederland, moet bijvoorbeeld niet via USA gaan. Dat soort zaken.

3.3 Bandbreedtes
Hier ligt niet de primaire focus van de reactie van het Forum. Voor de volledigheid zie de separaat toegestuurde opmerkingen van SURFnet en SIDN.

3.4 Technische eisen

#	Eis uit ON2013-document	Opmerking
1.04	De opdrachtnemer moet een extra hoge beschikbaarheid kunnen leveren op alle locaties in het levergebied.	'extra hoge beschikbaarheid' is niet duidelijk. Welke parameters en wat zijn de minimum waarden? Term komt verder niet terug.
1.06	Opdachtnemer dient SNMP-toegang tot eindapparatuur op de Aansluitpunten voor monitoring en het uitlezen van gebruiksstatistieken te ondersteunen.	Zie opmerkingen bij par. 2.5 onder 5.20 hierboven.
1.08	Opdrachtnemer dient IPv4 / IPv6 conversie te ondersteunen.	1. Wat wordt hier (echt) gevraagd van de ISP? 2. Relevante RFC's noemen.
1.09	Opdrachtnemer dient IPv6 te ondersteunen.	1. Zo duidelijk mogelijk maken dat dat geldt voor alle genoemde IP gerelateerde eisen. 2. Relevante RFC's noemen.
2.02	De opdrachtnemer dient het gebruik van het BGP4-protocol te ondersteunen voor de uitwisseling van de routeringsinformatie tussen het netwerk van de deelnemer en het netwerk van de opdrachtnemer in zowel een multihomed-AS- als stub-AS-situatie.	Relevante RFC's noemen. Ook 32 bits AS-nummers moeten worden ondersteund (RFC4893) bijvoorbeeld. Wellicht ook RPKI (RFC6480) vragen? Volgens SURFnet is het positief als een een provider zich met RPKI bezig houdt. Het is nog vroeg voor grootschalige implementatie. Wellicht een idee om in een aanbesteding RPKI als 'wens' of 'ter informatie' mee te nemen. Wordt dan niet per se gewogen. SURFnet heeft zoiets gedaan in paragraaf '2.4 Additional service features' van de RFP van SURFnet voor upstream Internet-connectiviteit.

#	Eis uit ON2013-document	Opmerking
2.03	De opdrachtnemer moet aansluiten op de huidige inrichting van de Border Gateway Protocol versie 4 (BGP-4) multihomed configuratie van de deelnemer (eigen RIPE AS).	1. Beter iets als: "De opdrachtnemer dient een multi-homed aansluiting voor deelnemer te ondersteunen op basis van het BGP-4 protocol, waarbij de deelnemer gebruik maakt van een eigen Autonomous System (AS) nummer." 2. Verwijzen naar relevante RFC's, zoals RFC 4271. 3. Maakt dit het mogelijk dat de overheid zelf gaar 'peeren' via bijv. de AMS-IX?
2.06	De opdrachtnemer biedt BGP-4 feed bestaande uit de volledige routering en een default gateway aan.	Kan IP-transit ook?
2.07	De opdrachtnemer is in staat om routefiltering reactief toe te passen.	Hoe verhoudt dit zich tot eis 2.04? Gaat dat niet over hetzelfde?
2.08	De opdrachtnemer dient op minstens 2 verschillende Internet Exchanges aangesloten te zijn.	1. Waaronder AMS-IX? 2. In praktijk geen probleem, maar waar komt de eis vandaan? Moet dat nog in verschillende landen zijn?
2.10	Het moet voor deelnemer mogelijk zijn om met twee opdrachtnemers redundante Internet Access-functionaliteit te realiseren.	Wordt hier "multi-homed" bedoeld? Wat kan een opdrachtnemer hier aan doen?

Ad 4. Levertijden, beschikbaarheid en beheer

4.3. Eisen op het gebied van beheer en organisatie

#	Eis uit ON2013-document	Opmerking
1.02	De opdrachtnemer verklaart dat hij - om de in dit document geëiste resultaten te leveren - de achterliggende (beheer)processen op orde heeft.	Hoe? ISO 27001, ISO 9001 e.d.?
8.08	Rapportages worden ten minste aangeleverd in ODF- of Excel-formaat.	Gaat het alleen om bewerkbare spreadsheets? Voor tekstdocumenten is de standaard PDF/A, dat zorgt voor duurzame toegankelijkheid, passend.
11.2	De opdrachtnemer dient haar beveiligingsbeleid te baseren op de meest actuele versies van de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002 of opvolgers hiervan, of een gelijkwaardige normering.	Moet aanvullend niet om de Baseline Informatiebeveiliging Rijk (BIR), die gebaseerd is op ISO27001/27002 en specifieker is, worden gevraagd?
11.3	De opdrachtnemer dient op verzoek jaarlijks een goedgekeurde Third Party Mededeling (TPM) door een EDP-auditor te overleggen over de opzet, het bestaan en de werking van beheer- en beveiligingsmaatregelen. Het normenkader voor deze TPM is gebaseerd op eis 11.2.	Is het een eis om gecertificeerd te worden tegen ISO/IEC 27001 door een door de RvA geaccrediteerde instelling? Zie: http://www.rva.nl/?p=cins0200&action=search&search_typecode=C&search_scopes=27001